AVP Inspector for WEB servers User guide

December 1999

Copyright © 1999 Kaspersky Lab Ltd. All rights reserved.

No part of this document may be reproduced, changed or transmitted in any form or by any form by any means, electronic, mechanical or photographic, for any purpose, without the express written permission of Kaspersky Lab Ltd. and reference to this document.

All product names referenced herein are trademarks of registered trademarks of their respective owners. Kaspersky Lab disclaims proprietary interest in the marks and names of others. Although Kaspersky Lab makes every effort to ensure that this information is accurate, Kaspersky Lab will not be liable for any errors or omission of facts contained herein.

Kaspersky Lab reserves the right to modify specifications cited in this document without prior notice.

Table of contents

1. AVP INSPECTOR FOR WEB-SERVERS 6
1.1 Main Functions and Features 6
1.2 Distribution Kit 6
1.2.1 Distribution Kit 6
1.2.2 License agreement 7
1.2.3 Registration Card 7
1.3 Information in the Book 7
1.3.1 Product Support 8

2. AVP INSPECTOR FOR WEB SERVERS INSTALLATION PROCEDURE 9
2.1 System requirements 9
2.2 Installation Procedure 9

3. AVP INSPECTOR FOR WEB SERVERS™ PRINCIPLES OF OPERATION 22
3.1 Tests Performed By AVP Inspector for Web Servers™ 22
3.2 Analysis Of Changes On Disk 22
3.2.1 What to do if AVP Inspector for Web Servers™ reports changes 23

4. LAUNCHING AND CONFIGURING AVP INSPECTOR FOR WEB SERVERS™ 24
4.1 Launching AVP Inspector for Web Servers™ And Command Line Options 24
4.2 AVP Inspector for Web Servers™ Main Window 26
4.2.1 Menu Items 28
4.2.2 Toolbar 29
4.3 AVP Inspector for Web Servers™ Profiles 29
4.3.1 The “Profiles” Tab 29
4.3.2 The “Startup” Tab 31
4.4 The "AVP Inspector for Web Servers Configuration" Dialog Box 32
4.4.1 The “Configuration” Tab 32
4.4.2 The “Extensions” Tab 34

4.4.3 The “Files” Tab 37
4.4.4 The “Reports” Tab 38
4.4.5 The “History” Tab 39
4.4.6 The “AVP” Tab 41
4.4.7 The “Excludes” Tab 42
4.4.8 The “Backup/Restore” Tab 43

5. WORKING WITH AVP INSPECTOR FOR WEB SERVERS™ 46
5.1 First launch of AVP Inspector for Web Servers 46
5.2 Custom folder inspection 46
5.2.1 How To Create Folder List 47
5.3 How To Create New Tables 48
5.4 The Disk Tests Summary Dialog Box 48
5.5 The View File/Directory List Dialog Box 49
5.6 View Files 50
5.7 View Test History 51
5.8 Launching AVP Inspector for Web Servers™ as Windows NT service. 51

6. MESSAGES ABOUT SUSPICIOUS CHANGES OR POSSIBLE VIRUS INFECTION 54
6.1 Warnings displayed upon completion of tests 54
6.2 Troubleshooting 55

7. WARNING AND ERROR MESSAGES 56
7.1 Run-Time error messages 56
7.2 AVP Inspector for Web Servers™ Startup And Run-Time Messages 57
7.3 Debugging registers test messages 58
7.4 Other messages 58

8. GLOSSARY 60

9. KASPERSKY LAB LTD. 65

Dear customer,

We are happy that you have chosen AntiViral Toolkit Pro (AVP), the world's best anti-virus defense, for protecting your computer against computer viruses. Kaspersky Lab's best anti-virus experts are working hard to provide you with this best-of-breed anti-virus solution and to face your strictest conditions. By choosing AVP you choose unbeatable anti-virus protection.

Kaspersky Lab always cares about their customers, providing them with an easy-to-use and high performance products with strong and comprehensive functionality. The highest possible level of anti-virus protection, highly intelligent heuristic code analyzer, support for the most wide-spread mail formats, virus detection inside archived and compressed files, powerful management tools – these are the main advantages you get with AVP. We provide you with the ultimate customer service: round the clock technical support, extensive information support, personal attention and immediate response to a new virus attack.

We appreciate the trust you have placed in our anti-virus products. We hope you will find our work effective and useful.

Kaspersky Lab. Team.

1. AVP Inspector for Web-servers

1.1 Main Functions and Features

AVP Inspector for Web Servers™ is additional utility for unauthorized changes on Web-site control which works under Microsoft Windows 95/98® or Microsoft Windows NT®.

AVP Inspector for Web Servers™ registers changes to prevent data structures on Web site from bad consequences. It can recover modified objects.

AVP Inspector for Web Servers™ reduces the time needed to scan a PC for viruses. After it has run, the **AVP** scanner needs to check only new files and those that have changed.
Main Features of AVP Inspector for Web Servers™

The main features of **AVP Inspector for Web Servers™** are:

- Works in Microsoft Windows 95, Microsoft Windows 98 or Microsoft Windows NT environments;
- True 32-bit multitasking GUI;
- Maintains a database of the results of previous checks;
- Supports OLE2 document structures (Word, Excel and Access documents);
- Ability of transmitting report by means of e-mail;
- Ability of the editing of checking area;
- Specific abilities for data checking on Web site (for instance checking the files with extensions .cgi, .asp etc);
- Opportunity of starting AVP as Windows NT service.

Software and Hardware Requirements.

1.2 Distribution Kit

1.2.1 Distribution Kit

The AVP distribution kit contains the following components.

- License Agreement;
- Sealed envelope containing AVP distribution diskettes;
- User Guide;
- Register card.
    - ***Before you unseal the envelope make sure to thoroughly review License Agreement.***

1.2.2 License agreement

License Agreement is a legal agreement between you (either an individual or a single entity) and the manufacturer (Kaspersky Lab Ltd.) describing the terms on which you may employ the purchased by you antivirus product. Make sure to peruse License Agreement! If you do not agree to the terms of LA, Kaspersky Lab is not willing to license the software product to you and you should return the unused product to your AVP dealer for a full refund, but make sure the distribution diskette envelope to be sealed.
If you unseal the envelope it means that you agreed to all the LA terms.

1.2.3 Registration Card

To register please fill a detachable coupon of the register card (your full name, phone, e-mail address) and mail it to the dealer (the address is specified on your AVP kit box) you purchased the kit from.
You may also e-mail your register information to sales@avp.ru. But in this case make sure to specify your message subject as «Registration». If your mail/e-mail address or phone number changed please notify the entity you have mailed the register coupon to.
If registered you will become the AVP registered user and will be provided with the product support and the antivirus base updates for the period of your subscription. Besides Kaspersky Lab provides AVP registered users with information on the company new products.

1.3 Information in the Book

This book contains information on how to install and manage AVP, explains basic concepts of the software product and the way it can be applied,

recommends on how to manage and change settings. This book doesn't describe installation procedure and operation concepts of the package.

1.3.1 Product Support

All the registered users are provided with the product support for the period of subscription.
If you register and purchase the subscription you will be provided with the following services for the period of your subscription:

- antivirus base weekly update;
- new versions provision;
- phone, e-mail or in-office advising on matters related to your AVP package;
- provision of information on the AVP line new products and on the worldwide newborn computer viruses.

For more information on Kaspersky Lab services refer to your README.TXT file

2. AVP Inspector for Web servers installation procedure

2.1 System requirements

The minimum system requirements for AVP Inspector for Web Servers™ are:

- IBM PC (or 100% compatible) running MS Windows® 95/98/NT;
- 8 Mb RAM or more (16 Mb recommended) for Windows®95/98, at least 16 Mb RAM for Windows NT® (32 Mb recommended);
- At least 1 Mb free disk space on the hard drive.

2.2 Installation Procedure

Before you begin installation we recommend that you make backup copies of the original distribution diskettes and install **AVP Inspector for Web Servers™** from these backup diskettes. Then if accidental damage to a diskette occurs you will be able to restore the damaged diskette from the original one.

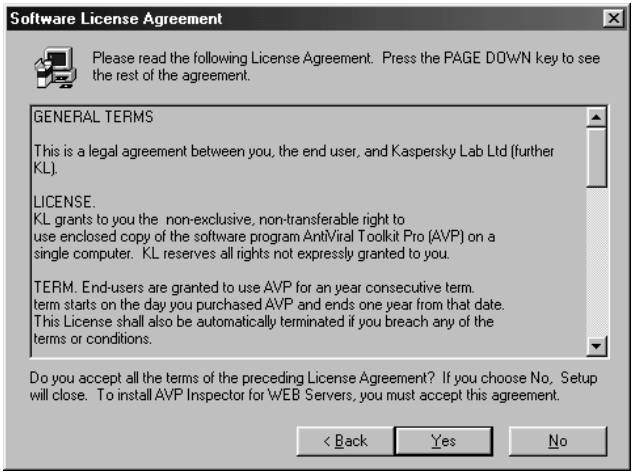
- Switch your PC on and boot Windows 95/98/NT.
- Insert the distribution diskette (or its backup copy) into the floppy drive.
- Run SETUP.EXE and follow the instructions on screen.

Welcome
INFORMATION PROTECTED
KASPERSKY
Welcome to the AVP Inspector for WEB Servers Setup program. This program will install AVP Inspector for WEB Servers on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Next >
Cancel

The Welcome to the AVP Inspector for Web Servers Window

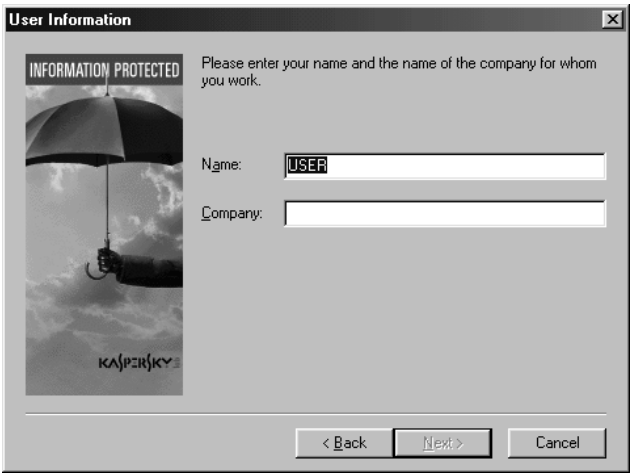
During the installation procedure you will be prompted for some information that is necessary to set up **AVP Inspector for Web Servers™** on your PC.

The installation program will prompt you to read the License Agreement. Read it carefully and, if you agree to all its conditions, continue Setup by pressing the "**Yes**" button. If you do not agree press the "**No**" button to abort the installation.


Software License Agreement
Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.
GENERAL TERMS
This is a legal agreement between you, the end user, and Kaspersky Lab Ltd (further KL).
LICENSE.
KL grants to you the non-exclusive, non-transferable right to use enclosed copy of the software program AntiViral Toolkit Pro (AVP) on a single computer. KL reserves all rights not expressly granted to you.
TERM. End-users are granted to use AVP for an year consecutive term. term starts on the day you purchased AVP and ends one year from that date. This License shall also be automatically terminated if you breach any of the terms or conditions.
Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install AVP Inspector for WEB Servers, you must accept this agreement.
< Back
Yes
No

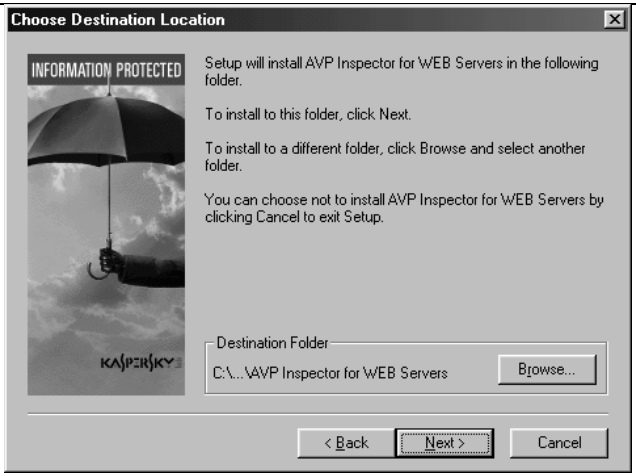
The License Agreement Window.

User Information. Next you must register your copy of **AVP Inspector for Web Servers™**. To do you must enter the required information (first and last names, company name, registration number) into the corresponding fields. Your registration number is printed on the registration card enclosed with the **AVP Inspector for Web Servers™** software.



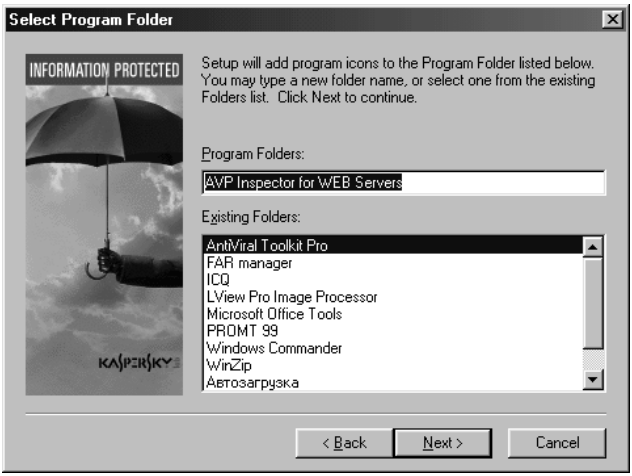
Registering your copy of AVP Inspector for Web Servers

Choose Destination Location. Now you should select the destination directory into which **AVP Inspector for Web Servers™** will be installed. If you want to install **AVP Inspector for Web Servers™** to a directory other than the default, press "**Browse**" button. From the "**Choose Directory...**" window select the directory into which you want to install the software.


Choose Destination Location
INFORMATION PROTECTED
Setup will install AVP Inspector for WEB Servers in the following folder.
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
You can choose not to install AVP Inspector for WEB Servers by clicking Cancel to exit Setup.
Destination Folder
C:\...\AVP Inspector for WEB Servers
Browse...
< Back
Next >
Cancel

Choosing the destination directory for AVP Inspector for Web Servers ™.

Select Program Folder. This option lets you specify the name under which the **AVP Inspector for Web Servers™** program and documentation files can be accessed from the Windows Start menu. You can change the group name by clicking on the input field and typing the desired name. You can place **AVP Inspector for Web Servers** into an existing program group by selecting the group name from the list.


Select Program Folder
INFORMATION PROTECTED
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.
Program Folders:
AVP Inspector for WEB Servers
Existing Folders:
AntiViral Toolkit Pro
FAR manager
ICQ
LView Pro Image Processor
Microsoft Office Tools
PROMT 99
Windows Commander
WinZip
Автозагрузка
< Back
Next >
Cancel

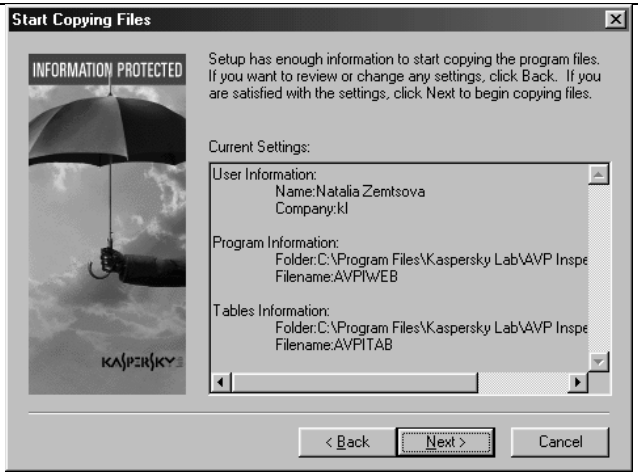
Selecting of program folder for AVP Inspector for Web Servers ™.

Setup Type**.** Next you will be prompted for the type of **AVP Inspector for Web Servers™** installation.

- **Typical** – recommended for most users. If you select Typical install installation you will be prompted only for the destination directory into which **AVP Inspector for Web Servers ™** is to be installed.
- **Custom** – recommended for advanced users. This option allows you to change other settings during installation.

Selecting the AVP Inspector for Web Service Setup Type.

Start Copying Files. If you selected **Typical** installation you will not be prompted for anything else. The installation program will now complete the installation of **AVP Inspector for Web Servers™**. You will see the current settings in the following window.

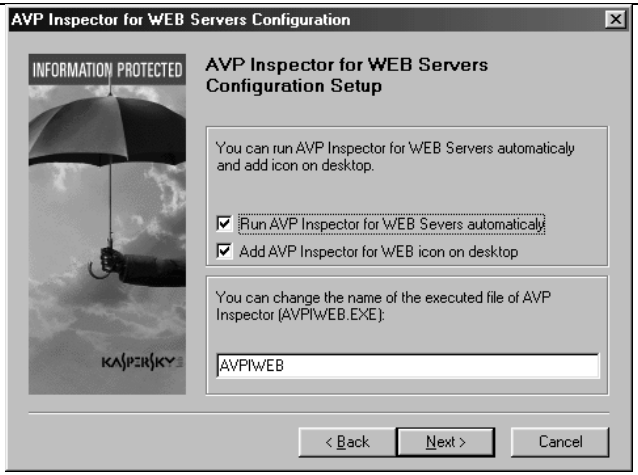

Start Copying Files
INFORMATION PROTECTED
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
User Information:
Name:Natalia Zemtsova
Company:kl
Program Information:
Folder:C:\Program Files\Kaspersky Lab\AVP Inspe
Filename:AVPIWEB
Tables Information:
Folder:C:\Program Files\Kaspersky Lab\AVP Inspe
Filename:AVPITAB
< Back
Next >
Cancel

Current settings of AVP Inspector for Web Servers ™

AVP Inspector for Web Servers Configuration**.** If you selected **Custom** installation you must complete four more steps to define configurations you need.

Step1. This step allows you to define:

- Run **AVP Inspector for Web Servers™** automatically: set up **AVP Inspector for Web Servers™** to launch automatically once a day during Windows start-up. This setting may be changed later, if required.
- Add an **AVP Inspector for Web Servers™** icon to the Desktop: this provides quick and convenient access to the program.
- Change the name of the **AVP Inspector for Web Servers™** executable (AVPIWEB.EXE): enter the filename you wish to use in the corresponding input field. (The filename you choose must have the extension EXE.)

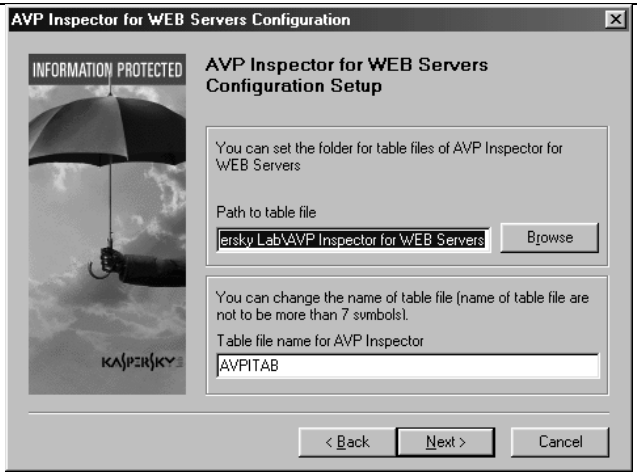

AVP Inspector for WEB Servers Configuration
INFORMATION PROTECTED
KASPERSKY
AVP Inspector for WEB Servers
Configuration Setup
You can run AVP Inspector for WEB Servers automaticaly and add icon on desktop.
Run AVP Inspector for WEB Severs automaticaly
Add AVP Inspector for WEB icon on desktop
You can change the name of the executed file of AVP Inspector (AVPIWEB.EXE):
AVPIWEB
< Back
Next >
Cancel

Configuration Setup 1

Step2. You can set the path to table file and change its name.

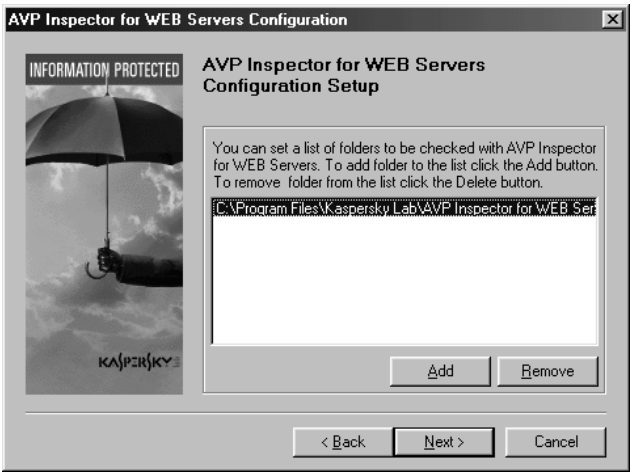
- Path to table files: the location where the table for the **AVP Inspector for Web Servers™** is placed. If this field is left empty the table will be placed in the root directory of the C: drive;
- Name of table file for **AVP Inspector for Web Servers™**.

🕮 **NOTE:** Table filename must not exceed 7 characters in length.


AVP Inspector for WEB Servers Configuration
INFORMATION PROTECTED
AVP Inspector for WEB Servers
Configuration Setup
You can set the folder for table files of AVP Inspector for WEB Servers
Path to table file
ersky Lab\AVP Inspector for WEB Servers
Browse
You can change the name of table file (name of table file are not to be more than 7 symbols).
Table file name for AVP Inspector
AVPITAB
< Back
Next >
Cancel

Configuration Setup 2

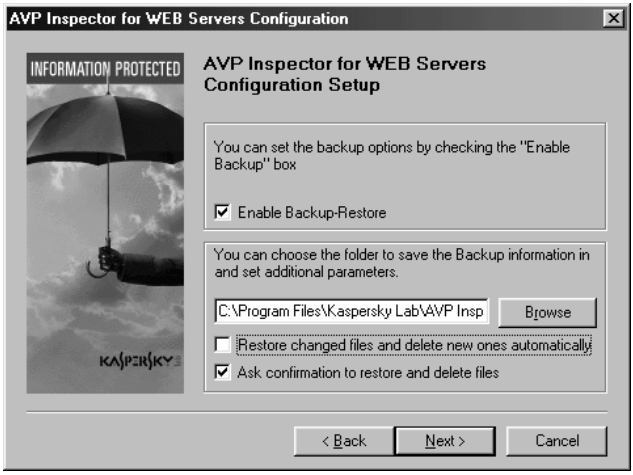
Step3. In following window you can set the list of folders to be checked with **AVP Inspector for Web Servers™.** Click the **ADD** button to add a folder to the list or the **Remove** button to delete it.


AVP Inspector for WEB Servers Configuration
INFORMATION PROTECTED
AVP Inspector for WEB Servers
Configuration Setup
You can set a list of folders to be checked with AVP Inspector for WEB Servers. To add folder to the list click the Add button. To remove folder from the list click the Delete button.
C:\Program Files\Kaspersky Lab\AVP Inspector for WEB Ser
Add
Remove
< Back
Next >
Cancel

Configuration Setup 3

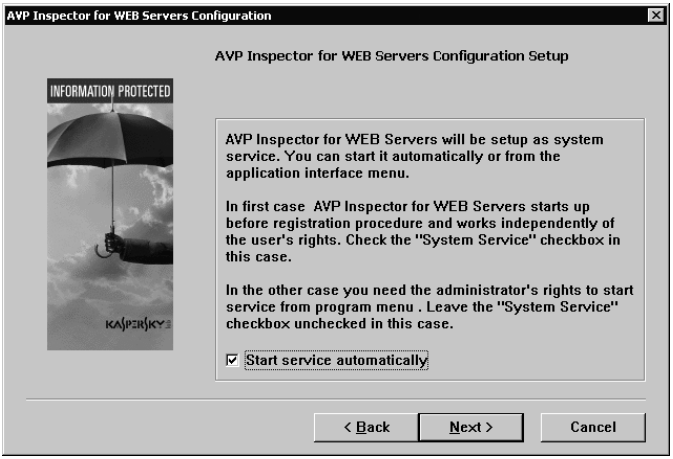
Step4. Next you set the backup options by checking the "Enable Backup-Restore" box and define the folder to save the backup information in. To restore changed files and delete new ones automatically check the appropriate box. You

can check the following box to the program ask your confirmation before restoring or deleting of files.


AVP Inspector for WEB Servers Configuration
INFORMATION PROTECTED
AVP Inspector for WEB Servers Configuration Setup
You can set the backup options by checking the "Enable Backup" box
Enable Backup-Restore
You can choose the folder to save the Backup information in and set additional parameters.
C:\Program Files\Kaspersky Lab\AVP Insp
Browse
Restore changed files and delete new ones automatically
Ask confirmation to restore and delete files
< Back
Next >
Cancel

Configuration Setup 4

Step5. In following window you should select the mode of start of **AVP Inspector for Web Servers™** as system service.

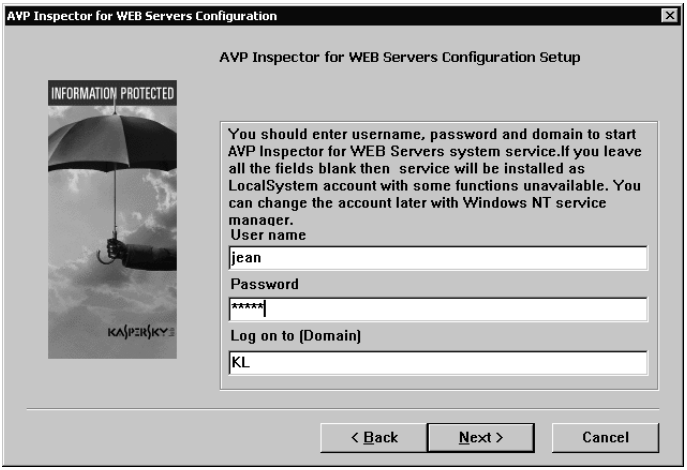

AVP Inspector for WEB Servers Configuration
AVP Inspector for WEB Servers Configuration Setup
INFORMATION PROTECTED
AVP Inspector for WEB Servers will be setup as system service. You can start it automatically or from the application interface menu.
In first case AVP Inspector for WEB Servers starts up before registration procedure and works independently of the user's rights. Check the "System Service" checkbox in this case.
In the other case you need the administrator's rights to start service from program menu . Leave the "System Service" checkbox unchecked in this case.
Start service automatically
< Back
Next >
Cancel

Starting of AVP for Web Servers as system service

If you check the box AVP Inspector for Web Servers will start up automatically before registration procedure and work independently of the user's rights. In the other case you can start system service manually from the program

menu and you must to have the administrator's right in this case.

Step6. You should enter username, password and domain to start **AVP Inspector for Web Servers™** system service. If you leave all the fields blank then service will be installed as LocalSystem account with some functions unavailable. You can change the account later with Windows NT service manager.


AVP Inspector for WEB Servers Configuration
AVP Inspector for WEB Servers Configuration Setup
INFORMATION PROTECTED
KASPERSKY
You should enter username, password and domain to start AVP Inspector for WEB Servers system service.If you leave all the fields blank then service will be installed as LocalSystem account with some functions unavailable. You can change the account later with Windows NT service manager.
User name
jean
Password
*****
Log on to (Domain)
KL
< Back
Next >
Cancel

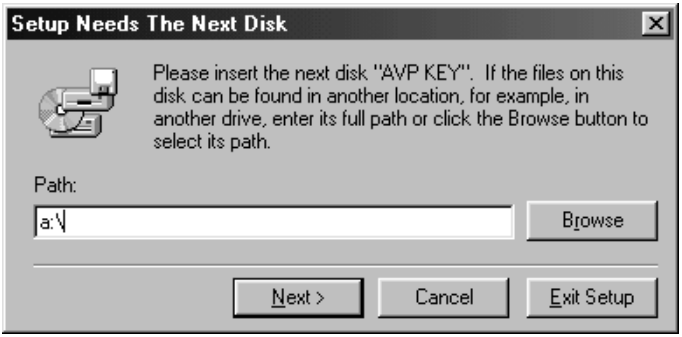
Enter username, password and domain

On completion of these steps the software is ready to be installed on your computer. You will see the "**Start Copying Files**" window. After you press the "**Next**" button, the installation program will begin copying program files to your computer.

📖 **NOTE:** Up to this point, if you wish to change a setting you may do so by pressing the "Back" button, which will take you back to the previous page of the installation settings. You can interrupt the installation any time by pressing the "**Cancel**" button. If you do this a warning message is displayed: **Are you sure you want to cancel installation?** If you press the "Yes" button the installation procedure will be cancelled. If you press "No", installation will continue.

If there is not enough free space on the destination drive to install the software the installation program will display a warning message. If this occurs, you may either abort the installation by pressing the "**Cancel**" button or free some space using Windows Explorer or a similar utility program and then resume the installation.

Setup Needs The Next Disk. Here you should specify the path to key file or press "**Browse**" button and select necessary directory. The key file is a file with key extension. It is your own key where you may find all auxiliary information necessary for operating of **AVP Inspector for Web Servers™.**


Setup Needs The Next Disk
Please insert the next disk "AVP KEY". If the files on this disk can be found in another location, for example, in another drive, enter its full path or click the Browse button to select its path.
Path:
a:\
Browse
Next >
Cancel
Exit Setup

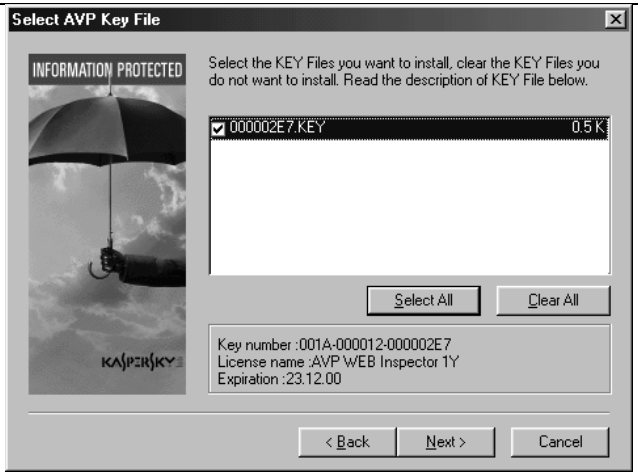
Defining of the key file path.

The key file contains several data.

1. Address, company name and phone of distributor of current version.
2. Support information.
3. Date of release.
4. Name and number of license.
5. Table of functionality of different components.
6. Period of availability of the license.

If you haven't this file in common folder of **AVP Inspector for Web Servers™** then program will operate as demo version.

Select AVP Inspector for Web Servers key file. By clicking left button select necessary key file. Moving cursor through the list you may see information about highlighted key file at the bottom of the window. If no key file is found then list will empty.

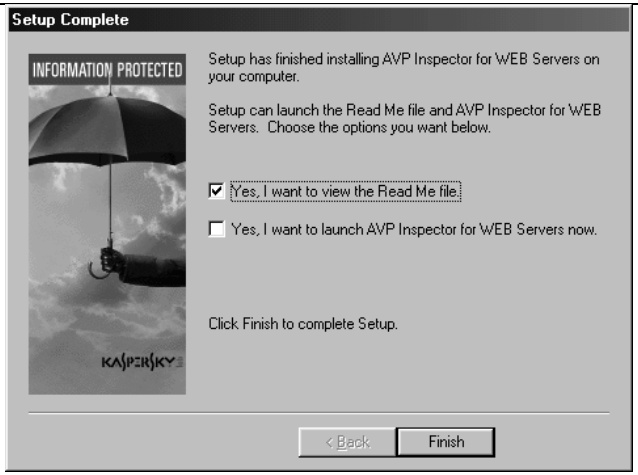

Select AVP Key File
INFORMATION PROTECTED
Select the KEY Files you want to install, clear the KEY Files you do not want to install. Read the description of KEY File below.
000002E7.KEY
0.5 K
Select All
Clear All
Key number :001A-000012-000002E7
License name :AVP WEB Inspector 1Y
Expiration :23.12.00
< Back
Next >
Cancel

Selecting the key file

After selecting of the key file click the "**Next**" button.

Setup Complete. In the follow window you will see window that offers to you to read file Readme and to launch the program after installation finish.

- Check the corresponding box to view Readme file.
- Check the box to start **AVP Inspector for Web Servers ™** after installation.


Setup Complete
INFORMATION PROTECTED
Setup has finished installing AVP Inspector for WEB Servers on your computer.
Setup can launch the Read Me file and AVP Inspector for WEB Servers. Choose the options you want below.
Yes, I want to view the Read Me file.
Yes, I want to launch AVP Inspector for WEB Servers now.
Click Finish to complete Setup.
KASPERSKY
< Back
Finish

Finishing of installation of AVP Inspector for Web Servers ™

Press the "**Finish**" button to close the installation program.

AVP.KEY File

The AVP.KEY file is a software key containing data that is required for the software to operate, such as:

- Dealer information;
- Support information;
- Product release date;
- Proof of registration;
- License validity period.

☞ **ATTENTION!** If this file is absent from the software's working folder, the software will behave as a demonstration version and some features will be disabled.

KEEP YOUR AVP.KEY FILE SAFE!!!

3. AVP Inspector for Web Servers™ Principles Of Operation

AVP Inspector for Web Servers™ works by calculating cyclic redundancy check (CRC) values for disk sectors and files, saving these values to a database (table) and then comparing the current CRC values with the previous values stored in the database. The database also holds additional information such as the size, creation and last modification dates of files, file attributes and data necessary to enable files that have changed (by being infected by a virus) to be repaired.

AVP Inspector for Web Servers™ also records and with each subsequent run checks certain significant operating system and hardware characteristics: the amount of available DOS memory and the number of installed hard drives. On each subsequent run the program checks that these values have not changed.

3.1 Tests Performed By AVP Inspector for Web Servers™

When **AVP Inspector for Web Servers™** is run for the very first time it saves the DOS memory size, the address of the INT 13h handler and creates tables for controlled drives.

During subsequent runs **AVP Inspector for Web Servers™** performs the following tests:

- the disk directory tree is verified. New and changed directories are scanned.
- files are checked. New, deleted, renamed, moved and modified files are scanned for changes in size, date and time of creation and last modification, and file CRC.

3.2 Analysis Of Changes On Disk

All the changes that are detected within files and disk sectors are analyzed and categorized as harmless or suspicious. **AVP Inspector for Web Servers™** provides information about all changes it detects. You can view this information in a dialog box or save it to disk for later viewing. In case of suspicious changes which may indicate the presence of a virus **AVP Inspector for Web Servers™** issues a virus attack warning.

The following changes are categorized as **suspicious**:

- changes in file contents where the file modification date and time remain the same (characteristic of most file viruses).
- different files have a similar size change.
- invalid date and time of last file modification, for example: day greater than 31, month greater than 12 or year greater than the current year; minutes greater than 59, hours greater than 23 or seconds greater than 59 (a common technique used by viruses to mark files that have been infected).
- changes in files listed as unchangeable (stable).
- changes characteristic of viruses that attack the DOS kernel (IO.SYS, IBMBIO.BIN files, etc.).

3.2.1 What to do if AVP Inspector for Web Servers™ reports changes

Always take note if **AVP Inspector for Web Servers™** reports changes to disk files or sectors, especially where it indicates suspicious changes. If the reason for these messages is unclear, it should be established. If program messages contain information that you don't understand, contact a qualified specialist or call AVP Technical Support for further information.

☞ **ATTENTION! Failure to heed warning messages increases the risk of a virus infecting your computer and the chances of data loss.**

4. Launching And Configuring AVP Inspector for Web Servers™

4.1 Launching AVP Inspector for Web Servers™ And Command Line Options

AVP Inspector for Web Servers™ can be launched using any standard for Windows method.

For example, it can be launched from the "AVP Inspector for Web Servers" program group which is created during the installation procedure. To do this, press the **Start** button, then select **Programs**, **AntiViral Toolkit Pro**, **AVP Inspector for Web Servers**, **AVP Inspector for Web Servers**. Another convenient way to start the program is by clicking on the AVP Inspector for Web Servers icon on the desktop.

🕮 **NOTE:** The name of the executable file of **AVP Inspector for Web Servers™** may be other than "AVPIWEB.EXE". If you chose a Typical installation the executable was given a random file name. However if you chose a Custom installation the executable file will have been given a name of your choice.

If you set "**Start AVP Inspector for Web Servers once per day"** in your AVPI profile, or during installation, **AVP Inspector for Web Servers ™** will launch automatically once every day, immediately after the operating system starts up.

If you run AVP from the command line you can set some additional options. The command line may look like this:

[Path]AVPIWEB.EXE [<options>] <drive> [<drive> ...]

Program Options (Command Line Parameters):

Program options are set using the command line. The option flags must begin with '-' or '/' and may be in upper or lower case.

-cl[<path>] causes test results to be appended to a file in the directory specified in <path>. For example, if you want to save the report to the AVP Inspector for Web Servers directory on drive C:, use the option: -clC:\AVPI\. If the option flag is not followed by a

	path name (e.g.: -cl) AVP Inspector for Web Servers will write the report to the root directory of the drive being tested. If a report file already exists, report data will be appended to it. You may use a long filename in <path> provided it is enclosed in quotes, for example -cl"c:\AVP Inspector for Web Servers". An alternative way to specify the location of the report file is by pressing the “Report” button in the View Test Results dialog box.
-hcl[<path >]	The same as previous key, but with HTML format of report.
-l[<path>]	causes test results to be written to a file in the directory specified in <path>. For example, if you want to save the report to the AVP Inspector for Web Servers directory on drive C:, use this option: -lC:\AVPI\. If the option flag is not followed by a path name (e.g.: -l) AVP Inspector for Web Servers will write the report to the root directory of the drive being tested. The new report will overwrite any previous report found in the specified directory. You may use a long filename in <path> provided it is enclosed in quotes, for example -l"c:\AVP Inspector for Web Servers".
-hl[<path >]	The same as previous key, but with HTML format of report**.**
-d	enables “Launch Once A Day” mode.
-d1	enables “Alternative Launch Once A Day” mode. In “alternative” mode tables are not updated and no results are displayed if no “suspicious” changes are found. The Test Results dialog box is displayed only if changes indicating possible infection by a virus are discovered.
-e	disables the Hidden attribute for table files.
-nl	disables disk locking (only when running under Windows 95/98)
-@<file>	enables logging of new and changed file names to a file named <file>. The AVP scanner may be used later to test these files for known viruses.
-ti<time>	enables the delayed launch feature. AVP Inspector for Web Servers will run <time> seconds after operating system start-up. The value of <time> may be from 1 to 999. This option may be useful if many programs are launched automatically when Windows 95® or Windows NT® start up.
-a<time>	defines the maximum period in seconds for which the Test Results dialog box should be displayed. The value of <time> can be from 1 to 999. This option is used only when running tests once a day.

-StopNNN this option allows certain tests to be disabled. The value of <NNN> is obtained from the sum of the following numbers:
8 - disable new directory scan;
16 - disable deleted directory scan;
32 -disable changed files scan;
64 - disable new files scan;
128 - disable deleted files scan;
256 -disable moved files scan;
512 - disable renamed files scan;
4096 - disable available DOS RAM size test.
So to exclude New Directory scan and New Files Scan, you should set this option to –Stop72

Example: If AVP Inspector for Web Servers is in the C:\AVP directory, and is to be launched once a day to scan C: and D: drives, reporting test results to the directory D:\TEMP, the command line you would use is: C:\AVP\AVPIWEB.exe -d -lD:\Temp\ C: D:

where:

C:\AVP\ is the name of the program directory;

-l option sets the directory for the test report to D:\Temp;

-d option ensures AVP Inspector for Web Servers runs only once a day;

C: and D are the drives to be tested.

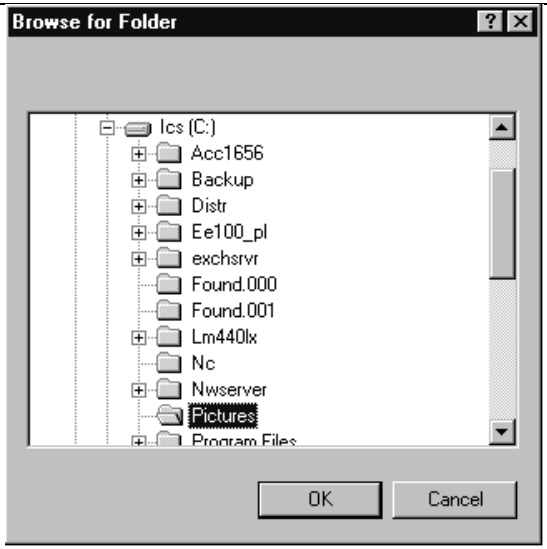
4.2 AVP Inspector for Web Servers™ Main Window

If AVP Inspector for Web Servers™ is launched without command line options it will run in dialog mode, i.e. the AVP Inspector for Web Servers main window will be opened.

AVP Inspector for Web Servers™Main Window

The main window contains the menu items: “File”, “Config”, “Scan”, “Help”, a toolbar and a list of the directories for scan.

You can edit the list of directories in the right-hand area of the main window. To add a new directory to the list to be tested click the “**Add**” button on the toolbar and choose a directory to scan in the opened window “Browse for Folder”.



The "Browse for Folder" Window

You cannot add the directory to the list for check, if it is parental or affiliated in relation to already available.

To remove a directory from the list, select it and click **"Delete"** button.

4.2.1 Menu Items

•**File -** exits the program.

•**Config:** change program settings, language, save current settings.

Configuration: displays the "AVPI Profiles" dialog box.

Switch to another language: if enabled, allows you to change the language used for menus and messages.

Save Config: saves the current program settings

Large Icons: toggles the size of the icons on the toolbar

•**Scan:** run tests on directories.

Scan Folders: runs tests.

Create New Table: creates new tables for directories.

Start AVPIWeb as Service: launches **AVP Inspector for Web Servers™** as service. In this case **AVP Inspector for Web Servers™** will work as Windows NT service.

Stop AVPIWeb as Service: stops service.

View scan history: views the results of previous test sessions.

•**Help**

Contents: launches the help system.
What's This? – obtain help for a selected element of the user interface.
Introducing: information about **AVP Inspector for Web Servers™**.
How to… how to perform key operations using AVP Inspector for Web Servers™
AVP Inspector for Web Servers™ On The Internet: go to the AVP Inspector for Web Servers™ Support Site on the Internet. This option opens your Web browser and requires an Internet connection.
About... displays information about the developers, the program version and your registration details. Click the "Support" button to see contact details for the Technical Support Service.
Version Information: displays versions of files included in AVP Inspector for Web Servers™ package.

4.2.2 Toolbar

The AVP Inspector for Web Servers toolbar contains the following buttons:

Exit the program;
Scan folders;
Display the "AVPI Profiles" dialog box;
Add folder to the scan list;
Delete selected folder from the scan list;
Display Help;
Stop scanning (this button is enabled only when tests are running).

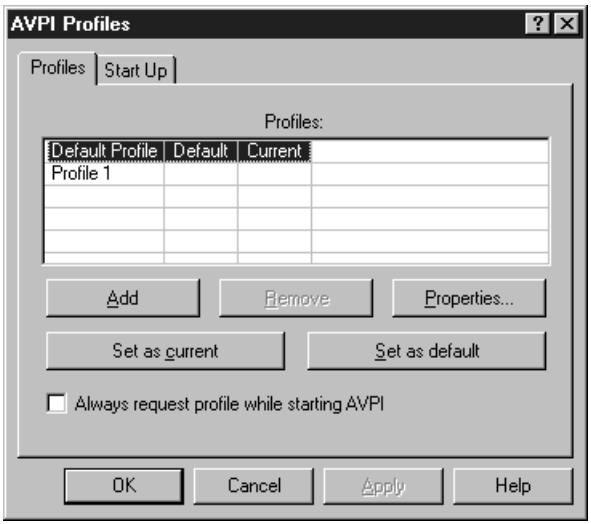
4.3 AVP Inspector for Web Servers™ Profiles

The **"AVPI Profiles"** dialog box may be opened from the AVP Inspector for Web Servers main window by pressing the button on the toolbar, or from the **"Configuration…"** menu item in the **"Config"** menu. This dialog box contains two tabs.

4.3.1 The "Profiles" Tab

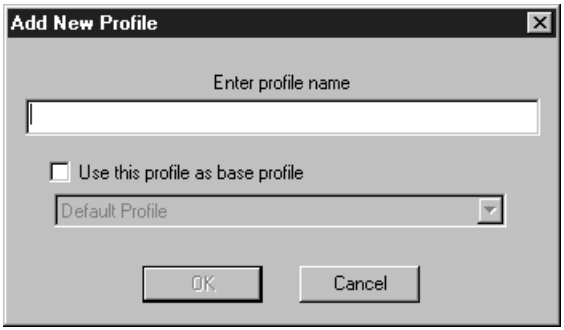
The **"Profiles"** tab is used to create and save sets of program settings which

are called profiles. When AVP Inspector for Web Servers™ is launched for the first time it creates a default profile called "Default Profile".



The "Profiles" Tab

To create a new profile, click the "**Add"** button. The **Add New Profile** dialog box will open. Under "**Enter profile name**" enter a name for the new profile. If you check "**Use this profile as a base profile**" you may use the drop-down list to select one of the existing profiles to use as a starting point for the new profile's settings.



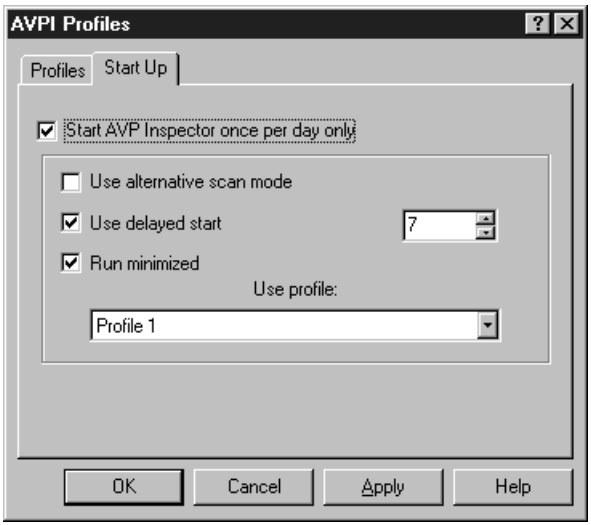
The "Add New Profile" dialog box

Any profile may be set as "current" – that is, used during the current AVP Inspector for Web Servers™ session – by selecting it from the list and clicking the "**Set as current**" button. One profile must be set as the default. This is the profile that will be loaded when AVP Inspector for Web Servers™ is launched. You set the default profile in the same way, by selecting one from the list and clicking the "**Set as default**" button.

A selected profile may be changed at the dialog "**AVP Inspector for Web Servers Configuration**" (*см. п. 4.4*), by clicking the "**Properties**" button. To delete a profile click the "**Remove**" button.

4.3.2 The "Startup" Tab

From the "Startup" tab you can change the settings that determine how AVP Inspector for Web Servers runs when it is launched automatically at start-up.



The "Startup" Dialog Box

"Start AVP Inspector for Web Servers once per day only"

By selecting this check box you ensure that AVP Inspector for Web Servers runs only once per day no matter how many times you restart your computer. This saves time when rebooting.

"Use alternative scan mode"

This mode disables the updating of tables and prevents further tests from running if no suspicious changes (indicating the likelihood of a virus infection) are found.

"Use delayed start"

This option allows you to specify an interval in seconds (between 1 and 999) which must elapse between startup and when AVP Inspector for Web Servers launches. This option can reduce the load on the system if AVP Inspector for Web Servers is just one of a number of programs that are all launched at start-up.

"Run minimized"

By setting this checkbox you can have AVP Inspector for Web Servers™ start minimized.

"Use profile"

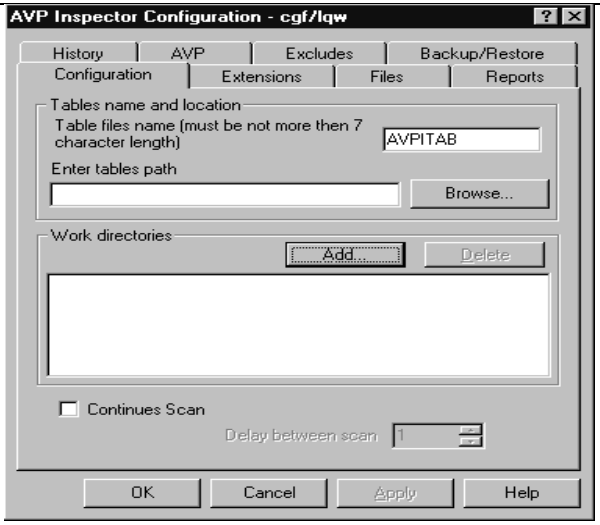
Using the drop-down list you can select a profile to use for once-a-day launches.

4.4 The "AVP Inspector for Web Servers Configuration" Dialog Box

To change the settings in a particular profile, select the profile you want to change in the **AVPI Profiles** dialog box (**Profiles** tab) and click the "**Properties**" button. The **AVP Inspector for Web Servers Configuration** dialog box will appear. This dialog box has nine tabs.

4.4.1 The "Configuration" Tab

The Configuration tab lets you specify some basic preferences about the way AVP Inspector for Web Servers runs.



The "Configuration" Tab

"Table name and location"

In these input fields you can specify the file name and path for table files.

📖 **NOTE:** The file name must not exceed 7 characters in length. The reason for this limitation is that a separate table file is created for each drive and an additional letter is appended to the specified name to indicate the drive letter. You may only specify 7 characters so that when the drive letter is added the resulting name is compatible with MS-DOS and its 8-character limit.

There is no need to specify a path name if you want the table files to be kept in the root directory of the tested drive. If for some reason this is undesirable you may specify a directory that will be used to store the tables for **all** the tested drives (except for A: and B: drives and other removable drives.

ATTENTION! If you specify a directory name it must also be in the MS-DOS compatible format so no name in the path may be longer than eight characters. To ensure this, use the "Browse" button when selecting which directory to use.

"Work directory"

In this field you can create a list of directories with contents that change frequently, which you want to exclude from testing. Press the **"Add"** button to add to the list a directory you want to exclude from testing. Highlight a directory

in the list and press the **"Remove"** button to remove it from the list.

📖 **NOTE:** Although AVP Inspector for Web Servers does not report changes in working directories, information about any changes is still passed to AVPIC.

"Continues Scan"

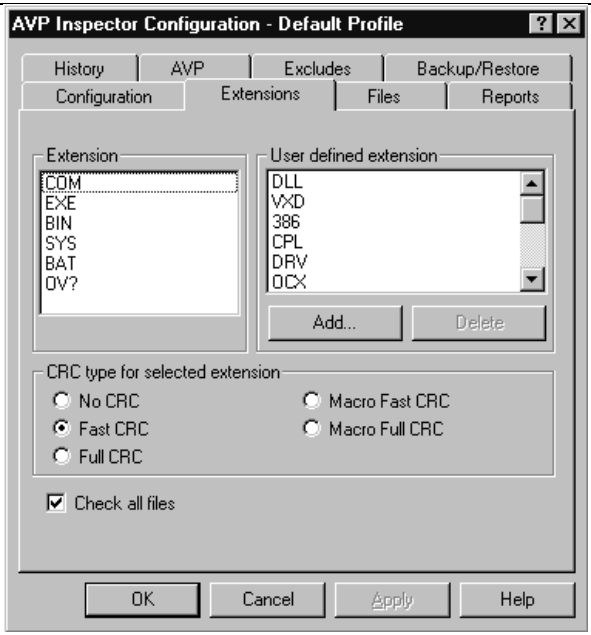
By checking this box you can run test in a mode of continuous scanning. Enabling this parameter the efficiency of operating increases but traffic of the Web-server greatly increases.

"Delay between scan"

To decrease traffic specify number of minutes to delay loading **AVP Inspector for Web Servers** you may determine this time according to your experience. This value must be between 1 and 3600 seconds.

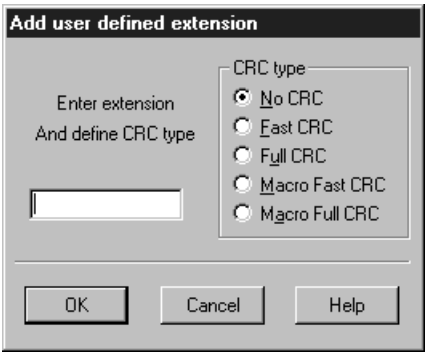
4.4.2 The "Extensions" Tab

The Extensions tab lets you specify the file extensions (file types) to be controlled by AVP and the type of check it performs on each one.



The "Extensions" Tab

The **"Extension"** list displays file extensions that will always be tested by AVP Inspector for Web Servers. Other file extensions can be added or removed from the **"User defined extension"** field.



Adding Additional Extensions

Press the **"Add"** button to add an extension to the list. The "**Add user defined extension**" dialog box will appear. To add a file type to the list of files that will be checked for changes by AVP Inspector for Web Servers enter its file

extension in the input field and click a radio button to select the type of check (No CRC, Fast CRC, Full CRC, Macro Fast CRC, Macro Full CRC) you want to use for it.

📖 **NOTE:** The "?" wildcard may be used in user-defined extensions. For example, by specifying OV?, AVP Inspector for Web Servers™ will test files with extensions of OVL, OVR etc.

The type of check specified in the **"CRC check for selected extension"** field is as follows:

- **No CRC check:** no CRC check is performed on files with this extension. Only the file size, time and date of creation is saved to the table.
- **Fast CRC check:** the check is dependent on the internal structure of the executable file. It combines reliable file validity control with minimal calculation time. This type of check is strongly recommended for COM, EXE, VXD, DLL, 386, CPL, SCR and other executable files.
- **Full CRC check:** a CRC is calculated based on the contents of the entire file. This type of check provides the most complete control over file validity, but requires a much greater calculation time. It is recommended for BAT and SYS files.
- **Macro Fast CRC check:** this check is dependent on the internal structure of the document file (such as Microsoft Word®, Microsoft Excel® and Microsoft Access® documents) and allows reliable file validity control for OLE2 documents. It is recommended for files with DOC, DOT (DO?), XLS, XLA, (XL?) and MDB extensions.
- **Macro Full CRC check:** a CRC is calculated on all of the macros contained within a document file. This type of check provides the most complete file validity control for OLE2 documents.

📖 **NOTE:** Macro CRC checks are recommended only for OLE2 format files that may contain macros. So far the following applications are supported: Microsoft Word®, Microsoft Excel® and Microsoft Access®.

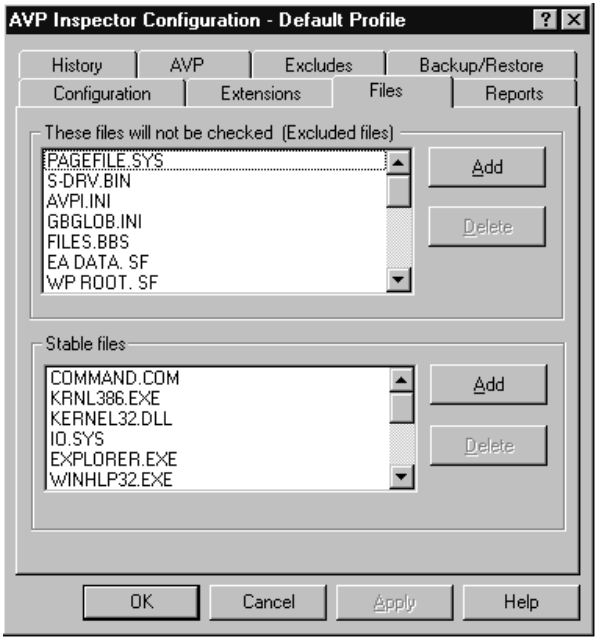
"Check all files"

By checking this box you can choose to have all files checked for changes. If you choose this option the **"User defined extension"** window will display an

extra line called ***"Other Files".*** For files not listed in **"Extension"** or **" User defined extension "** the type of CRC check to use can be set.

4.4.3 The "Files" Tab

From the Files tab you can view and edit the lists of stable files and excluded files, and set the parameters that determine whether a change in file size should be considered dangerous.



The "Files" Tab

"These files will not be checked (Excluded files)"

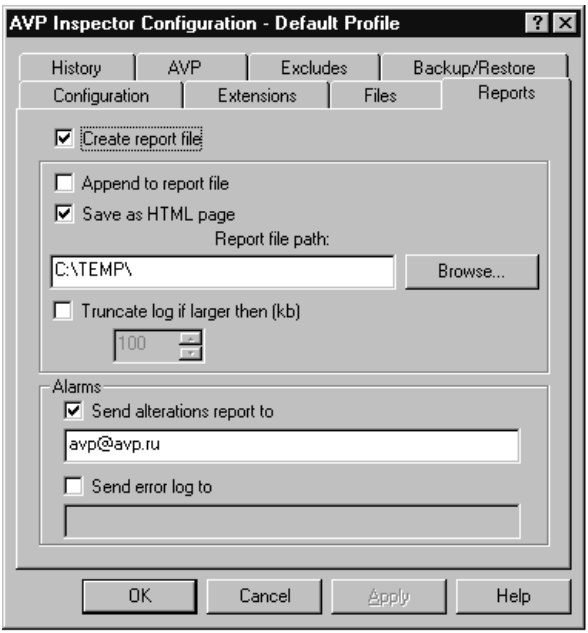
This is a list of files that will not be tested. Usually the files that are listed here are those that are constantly being modified by the operating system or some other software. Windows 95/98/NT swap files are examples of such files. By adding their names to this list you will not receive unnecessary warnings. To add a file to this list press the **"Add"** button and select a file using a standard file selection dialog box. To remove a file from the list, select it and click **"Delete"**.

"Stable files"

This is a list of files which should not change under any circumstances. Examples of such files are the command shell (Command.Com, NDos.Com, etc) operating system kernel files (IO.SYS, IBMBIO.COM), various trap files. To add a file to this list press the **"Add"** button and select a file using a standard file selection dialog box. To remove a file from the list, select it and click **" Delete "**.

4.4.4 The "Reports" Tab

From the "**Reports**" tab you can specify whether you want AVP Inspector for Web Servers to create a report of its actions and test results, choose the location of the report files and specify whether new reports are to be appended to existing reports or to overwrite the existing file.



The "Reports" Tab

"Create report file"

If this box is checked then upon completion of tests a report file will be created for each tested drive.

"Append to report file"

If this box is checked and a report file already exists, new data will be appended to it. If this box is unchecked, the old report file will be overwritten by the new one.

"Save as HTML page"

In this case all reports will be saved at HTML format.

"Report file path:"

In this field you specify the directory in which report files will be saved. You may use long filenames here as long as you enclose them in quotes, for example "c:\AVP Inspector for Web Servers". However, the best way to select the path is to use the "**Browse**" button.

"Truncate log if larger then (kb)

This check enables a user to limit the report file size. The value (Kb) can be entered in the below text field (the default value is 500 Kb).

"Alarms"

In these fields you can specify E-mail addresses to sent alterations reports and error logs.

4.4.5 The "History" Tab

This tab allows you to change the settings that determine whether historical information about disk tests is kept.

The "History" Tab

"Save check history information"

If this box is checked, historical records will be saved to the history database.

"Save History Info only at first check"

If this box is checked, only the history of the first check of the day will be saved.

"Save History Info at all checks"

If this option is selected, the history of each check will be saved.

The quantity of history information that is stored can be limited in two ways: by restricting the number of records to keep or by restricting the number of days' information to keep.

"Check Max Number"

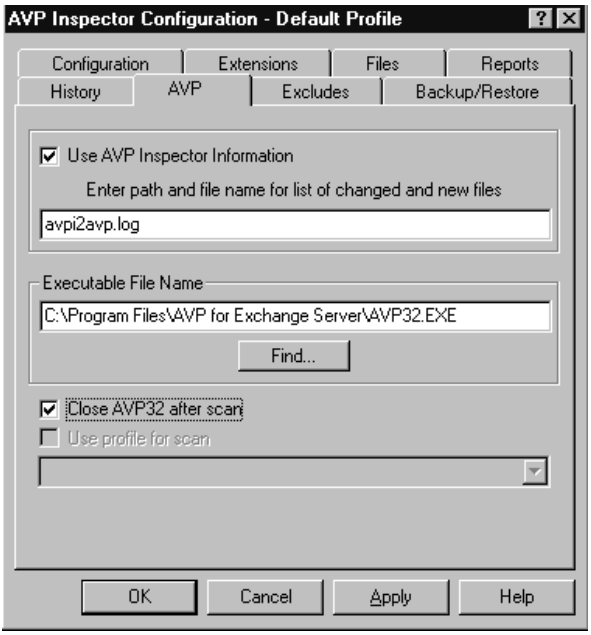
If you select this option you can then specify the maximum number of records you want to keep in the history database.

"Check Days"

If you select this option you can then specify the maximum number of days' information to keep in the history database.

4.4.6 The "AVP" Tab

Using this tab you can view and edit the settings that control operation of the virus scanner AVP® for Windows, and set the path and name of the file in which AVP Inspector for Web Servers™ will store the names of new and changed files for subsequent virus scanning.



The "AVP" Tab

"Use AVP Inspector for Web Servers information"

AVP Inspector for Web Servers™ can create a list of files to be checked by

the virus scanner. This list may contain the names of new, changed, renamed and moved files. In this field you can specify the full path and name of the file to be created. If only the file name is entered it will be created in the AVP Inspector for Web Servers™ home directory.

"Executable File Name"

In this field you enter the path and file name of the virus scanner AVP® for Windows. If you did not rename the AVP® for Windows executable (in other words, if it is called avp32.exe), clear the input field and use the **"Find"** button to locate it on all available local drives. If the name of the virus scanner executable file is not avp32.exe, enter the name into the input field and then click "Find" to determine the full path..

"Close AVP32 after scan"

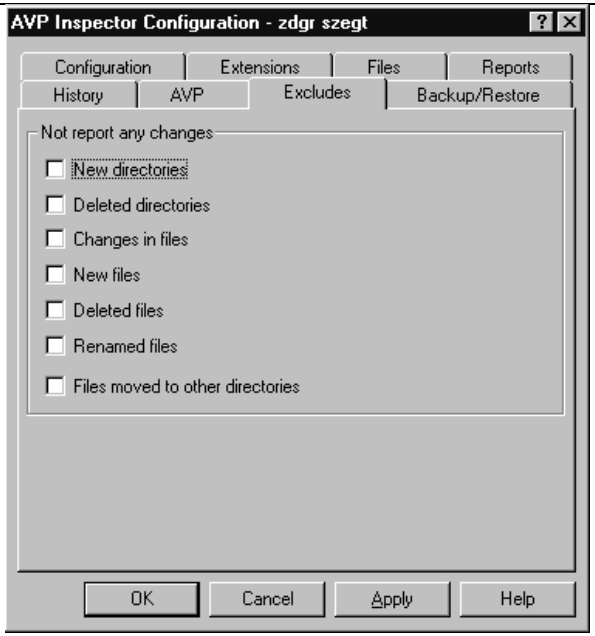
If this box is checked, the scanner window will close after completion of the virus scan.

"Use profile for scan"

AVP® for Windows supports multiple profiles. If you want AVP for Windows to use a profile other than the default when scanning files in the list created by AVP Inspector for Web Servers™, check this box and select the profile you wish to use from the drop-down list.

4.4.7 The "Excludes" Tab

This tab allows you to disable some of the tests that are normally performed by AVP Inspector for Web Servers.



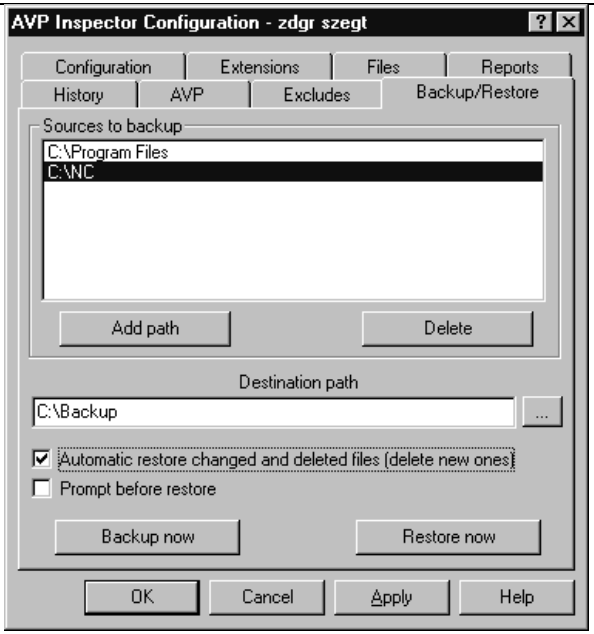
The "Excludes" Tab

A number of check boxes are displayed. If a box is checked, changes in the corresponding item will not be reported. The checks you can exclude are:

- New directories;
- Deleted directories;
- Changes in files;
- New files;
- Deleted files;
- Renamed files;
- Moved files.

4.4.8 The "Backup/Restore" Tab

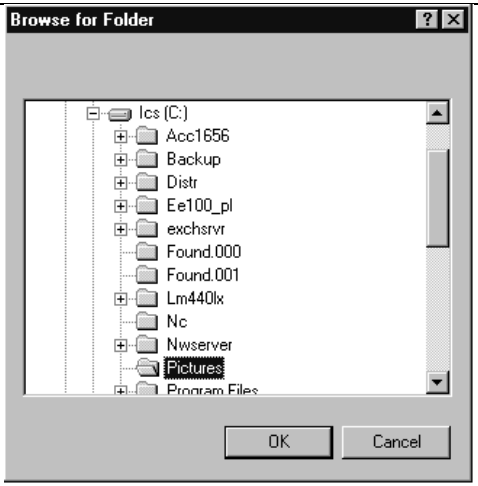
There is an opportunity of preservation of directories and their subsequent restoration in case of necessity for increase of safety of Web server work.



The "Backup/Restore" Tab

"Sources to backup"

In this field you specify the directories you want to save. To add a new folder to the list click the "**Add path**" button and choose the directory you need in the "**Browse for folder** " window.



The "Browse for Folder" Window

"Distination path"

In this field you can enter the path where your sources will be kept.

"Automatic restore changed and deleted files"

If this box is checked the **AVP Inspector for Web Servers™** restores the specified folders automatically if in them there were any changes.

"Prompt before restore"

If this box is checked the **AVP Inspector for Web Servers™** asks the sanction to restoration each time before that how to make actions.

🕮 **NOTE:**

- In case of the automatic restoring of complex structure of directories with subdirectories the program restore all of them step by step after several checks only. Therefore, if the continuous mode of check and the automatic restoration not are included, that such directory will not be restored completely.
- At removal of the catalogue from the list the catalogues with a backup copy do not leave automatically, that you should remove them manually.

5. Working With AVP Inspector for Web Servers™

5.1 First launch of AVP Inspector for Web Servers

When launched for the very first time, AVP Inspector for Web Servers™ automatically creates tables for all directories, which were given during installation to be tested (see **AVP Inspector for Web Servers™ Installation Procedure**).

If these table were not created you will see notification:

AVP Inspector
Cannot open tables file for drive H (H:\AVPITABH.DAT). No tables may have been created yet.
Create new table?
Yes
No

Reply "Yes" and all necessary tables will be created.

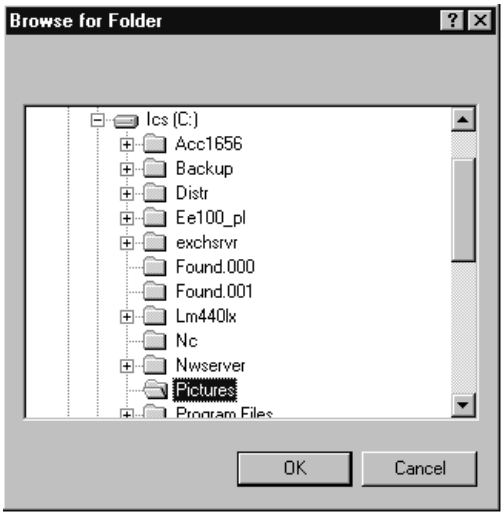
5.2 Custom folder inspection

If during installation you specified that the program should run once a day, this will happen the first time the operating system is loaded each day. AVP Inspector for Web Servers™ will launch automatically and will check folders for possible changes (see **AVP Inspector for Web Servers™ Operating Principles** for more detail.).

AVP Inspector for Web Servers™Main Window

5.2.1 How To Create Folder List

First you should decide what folders you want to test. Click the ADD button on toolbar and choose folder in opened window “Browse for folder”.



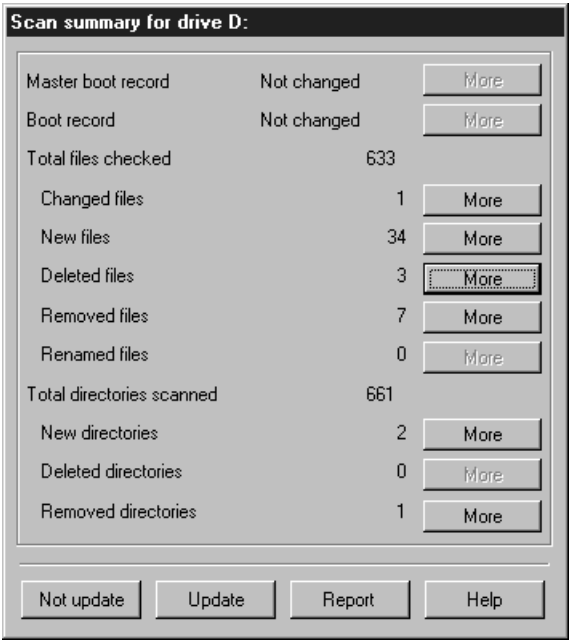
The “Browse for folder” window.

To add the other folder to folder list repeat this actions one more time.

5.3 How To Create New Tables

To create new table click **"Scan"** in the main menu, then **"Create New Tables"**.

5.4 The Disk Tests Summary Dialog Box



The "Scan summary for drive" Dialog Box

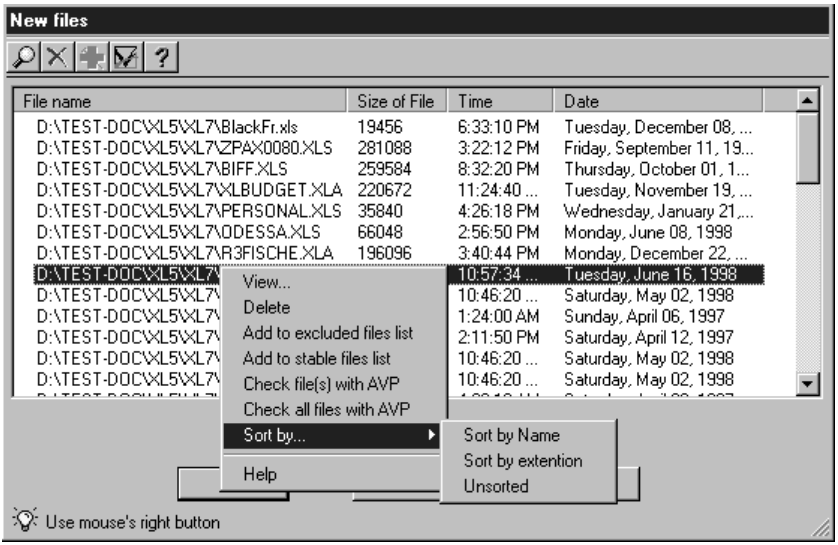
This dialog box displays a summary of changes since the last disk test. Information shown includes: the numbers of changed, deleted, renamed, moved and new files, new and deleted directories; also information about changes to the master boot sector and boot sector. For detailed information about these objects press the **"More"** screen button for the desired object type.

To create a report press the **"Report"** button. AVP Inspector for Web Servers™ will prompt you for a report file name and then save the report data to this file.

To update tables to reflect these changes press the **"Update"** button. If you

don't want to update the tables press the **"Not update"** button or the **"Esc"** key.

5.5 The View File/Directory List Dialog Box


New files
File name
Size of File
Time
Date
D:\TEST-DOC\XL5\XL7\BlackFr.xls 19456 6:33:10 PM Tuesday, December 08, ...
D:\TEST-DOC\XL5\XL7\ZPAX0080.XLS 281088 3:22:12 PM Friday, September 11, 19...
D:\TEST-DOC\XL5\XL7\BIFF.XLS 259584 8:32:20 PM Thursday, October 01, 1...
D:\TEST-DOC\XL5\XL7\XLBUDGET.XLA 220672 11:24:40 ... Tuesday, November 19, ...
D:\TEST-DOC\XL5\XL7\PERSONAL.XLS 35840 4:26:18 PM Wednesday, January 21,...
D:\TEST-DOC\XL5\XL7\ODESSA.XLS 66048 2:56:50 PM Monday, June 08, 1998
D:\TEST-DOC\XL5\XL7\R3FISCHE.XLA 196096 3:40:44 PM Monday, December 22, ...
D:\TEST-DOC\XL5\XL7\ 10:57:34 ... Tuesday, June 16, 1998
D:\TEST-DOC\XL5\XL7\ 10:46:20 ... Saturday, May 02, 1998
D:\TEST-DOC\XL5\XL7\ 1:24:00 AM Sunday, April 06, 1997
D:\TEST-DOC\XL5\XL7\ 2:11:50 PM Saturday, April 12, 1997
D:\TEST-DOC\XL5\XL7\ 10:46:20 ... Saturday, May 02, 1998
D:\TEST-DOC\XL5\XL7\ 10:46:20 ... Saturday, May 02, 1998
View...
Delete
Add to excluded files list
Add to stable files list
Check file(s) with AVP
Check all files with AVP
Sort by...
Help
Sort by Name
Sort by extention
Unsorted
Use mouse's right button

The View File/Directory List Dialog Box.

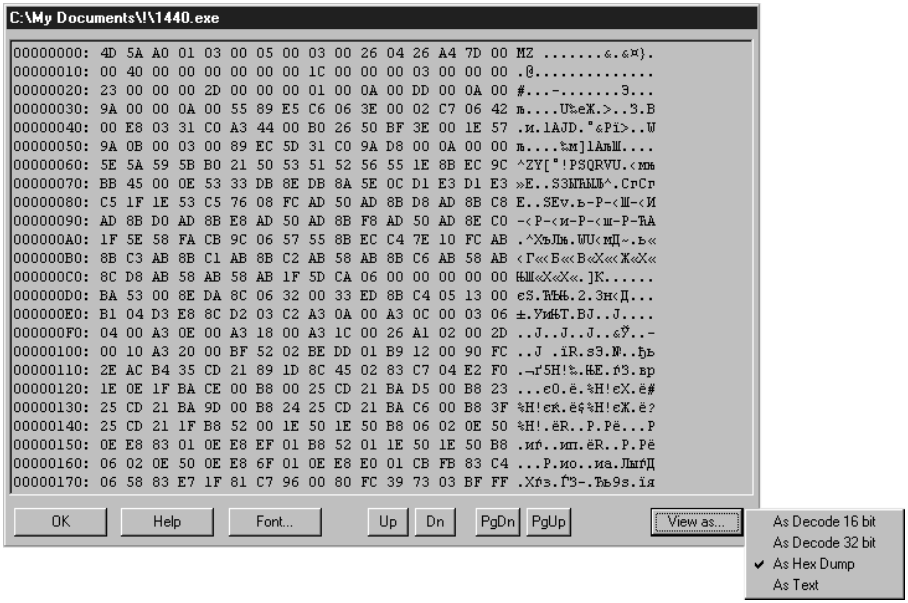
🕮 **NOTE:** suspiciously changed files are tagged with this symbol: ☹.

Using the toolbar, or by right-clicking an item and using the context menu, you can:

- View a file or directory contents (**View…,**);
- Add a file to the excluded files list (**Add To excluded files list**);
- Add a file to the stable files list (**Add to stable files list**);
- Delete a file (**Delete,**);
- Check a file for infection by known viruses using AVP® (**Check file(s) with AVP,**)

List of files can be sorted: **Sort by name**, **Sort by extension**, **Unsorted**.

5.6 View Files

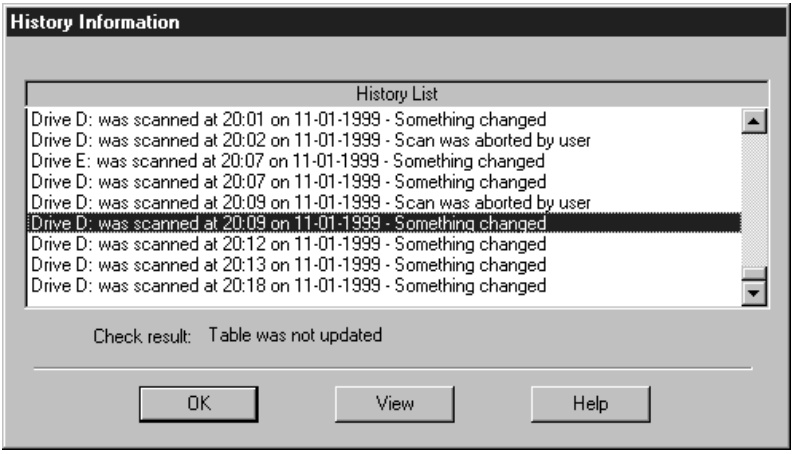


View Files Dialog Box

This dialog box is displayed if you press the "**View**" button in the file/directory view dialog box or if you select the "**View**" menu item from the context menu in this dialog box.

- **PgUp**, **PgDn**, **Up**, **Down:** these buttons allow you to navigate within the file being viewed.
- **View as…:** this button lets you change the view mode. You may choose from the following modes: 16-bit assembly language (to view DOS files), 32-bit assembly language (to view Windows executable files), hex view and text view.

5.7 View Test History


History Information
History List
Drive D: was scanned at 20:01 on 11-01-1999 - Something changed
Drive D: was scanned at 20:02 on 11-01-1999 - Scan was aborted by user
Drive E: was scanned at 20:07 on 11-01-1999 - Something changed
Drive D: was scanned at 20:07 on 11-01-1999 - Something changed
Drive D: was scanned at 20:09 on 11-01-1999 - Scan was aborted by user
Drive D: was scanned at 20:09 on 11-01-1999 - Something changed
Drive D: was scanned at 20:12 on 11-01-1999 - Something changed
Drive D: was scanned at 20:13 on 11-01-1999 - Something changed
Drive D: was scanned at 20:18 on 11-01-1999 - Something changed
Check result: Table was not updated
OK
View
Help

The "History Information" Dialog Box

This dialog box allows you to view the results of previous tests. The **"Result"** field displays table update information. The **"Test List"** field displays information about changes on the tested drive, or about the type of test, for example: "Creation Of Tables" or "Active Stealth Virus Test". If any changes were detected you can view the test results by pressing the **"View"** screen button. The standard Test Results dialog box will then be displayed.

5.8 Launching AVP Inspector for Web Servers™ as Windows NT service.

During installation of the program you can choose a mode of start **AVP Inspector for Web Servers™** as a system service. In this case **AVP Inspector for Web Servers™** will start automatically with computer boot and check chosen folders. Also **AVP Inspector for Web Servers™** uses profile set as default and the tables, which are created automatically during first start of GUI part of **AVP Inspector for Web Servers™** for the directories, specified by you during installation.

If the continuous scanning was not specified in a mode of automatic start of a system service, after test of the given area **AVP Inspector for Web Servers™** is unloaded after scan. In case you didn't specify run **AVP Inspector for Web Servers™** as system service during installation you able to start **AVP Inspector for Web Servers™** service manually.

To launch **AVP Inspector for Web Servers™** as system service manually click **"Scan"** in the main menu, then **"Start AVPIWeb as Service"**. The main window gets the following kind:

AVP Inspector for Web Servers™Main Window

In this case it will work with the current profile.

If you want to change a profile configuration you should restart **AVP Inspector for Web Servers™** as a service after changing.

To stop work **AVP Inspector for Web Servers™** as a service part, press the "**Stop service**" button.

In case of detection of any suspicious changes in tested area the **AVP Inspector for Web Servers™** restores the specified folders automatically if the mode of automatic restoration of folders is determined.

The reports and error logs are sent by mail to addresses specified in a bookmark **"Report"** of profile properties.

The user, which registration record is set at installation **AVP Inspector for Web Servers™** and be used for start of a system service should to have the appropriate rights. By default such rights in Win NT have all users, included in local manager group. The user, which registration record gets out for start of a service part, should have entered MAPI profile on given local machine.

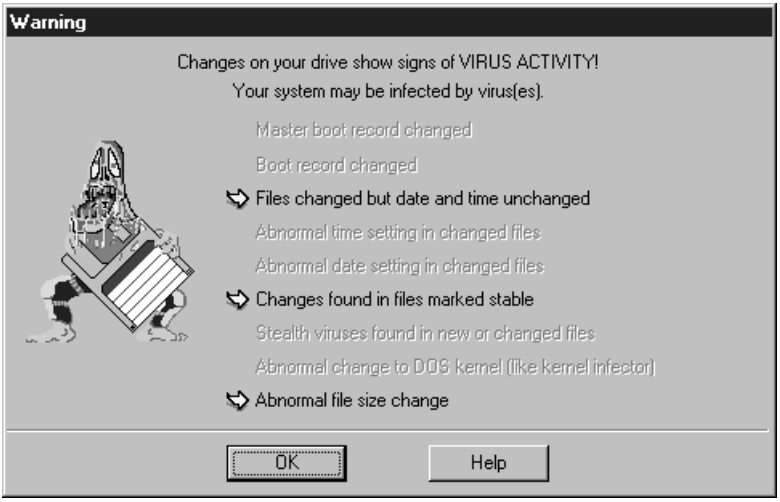
The event viewer reflects the information about mistakes of service start or

sending of mail.

6. Messages about suspicious changes or possible virus infection

6.1 Warnings displayed upon completion of tests

Upon completion of tests, and if changes that indicate the possible presence of viruses have been detected, AVP Inspector for Web Servers™ displays a dialog box with the list of the suspicious changes.


Warning
Changes on your drive show signs of VIRUS ACTIVITY!
Your system may be infected by virus(es).
Master boot record changed
Boot record changed
Files changed but date and time unchanged
Abnormal time setting in changed files
Abnormal date setting in changed files
Changes found in files marked stable
Stealth viruses found in new or changed files
Abnormal change to DOS kernel (like kernel infector)
Abnormal file size change
OK
Help

Changes are considered suspicious in these cases:

- **Files changed but date and time unchanged** - changes in file contents, not accompanied by changes in the date and time of last modification, generally indicate the presence of a file virus.
- **Abnormal time setting in changed files**- an invalid time of last modification in changed files: number of minutes greater than 59, number of hours greater than 23 or number of seconds greater than 59, can indicate the presence of a file virus. (Some viruses use this method to "tag" infected files).
- **Abnormal date setting in changed files** - an invalid date of last modification in changed files: day value exceeds 31, month value exceeds 12 or year value exceeds current year, can indicate the presence of a file virus. (Some viruses use this method to "tag" infected files).

- **Changes found in files marked stable** - a file listed as stable (should not change) has changed. Unless you know of a good reason why the file(s) listed have changed (for example, you have installed an updated version of the operating system) these changes are likely to be due to infection by a virus.
- **Abnormal file size change** - The size of several different files has changed by a similar number of bytes. This could be the result of a file virus which has infected each of these files.

6.2 Troubleshooting

Operating notes about AVP Inspector for Web Servers™

Possible problems which may occur while running AVP Inspector for Web Servers are:

- Error opening physical drive 0 (80h) may occur (under Windows NT® only). This may occur when Norton System Doctor is running and the IDE bus mastering drivers by Intel version 1.75, 10/14/96 are installed. To avoid this error close down Norton System Doctor or install other drivers. (No problems are known with version 1.68 or with standard drivers.)

If you come across any errors or erratic behaviour of AVP Inspector for Web Servers™ under certain conditions, please report them to AVP Technical Support (for example, via e-mail: support@avp.ru).

7. Warning and error messages

7.1 Run-Time error messages

"Cannot allocate memory"

This message may appear if there is not enough memory for AVP Inspector for Web Servers™ to complete some operation.

"Cannot open AVPITABX.DAT"

where X is a drive letter. This message means that it is impossible to open the specified table file. (Note that the name can be changed at installation time or using the Configuration dialog).

This message may be caused by several reasons. Tables on X: drive may not have been created. To correct this problem you should create the tables. Also check the table name setting. If you changed this setting, check if the tables with this name exist. If not, recreate the tables.

"AVPITABX.Dat table file already exists. Overwrite the tables?"

This message may appear if an attempt is made to create tables for a drive with already existing tables. As explained above, the table file name may be other than AVPITABX.DAT.

"The existing AVPITab.Dat file is incompatible with this version of AVP Inspector for Web Servers. Please create new table file."

This message may appear if you have updated AVP Inspector for Web Servers™ to a newer version. Newer versions of AVPI may use a different table file format. In this case you should recreate the table file.

"CRC error in table file. Be careful testing drive X:. AVP Inspector for Web Servers™ operation may be disrupted!"

Before running any tests, AVP Inspector for Web Servers™ checks the validity of each table file. If changes are found this message is displayed. If you see this message try to find the reason for the changes in table files. It is recommended that you recreate the tables for this drive to eliminate this error.

"Cannot create report file "

"Error writing report "

These messages are displayed if you choose an invalid name for the report file, if you attempt to save the report file to a write protected diskette, or if there is not enough disk space to save the report file.

"Error writing tables "

This message is displayed if you attempt to save a report file to a write protected diskette or if there is not enough disk space.

"Read error on drive X:"

This message is displayed if the program could not read a disk sector during tests. Try restarting the program. If the error persists, check your hard drive for errors.

"Too many directories on disk!"

This message is displayed if there is not enough memory for AVPI to build its internal data structures. During testing, AVPI builds tables representing the disk structure in memory to ensure high speed. The size of these tables is limited by the memory size of your computer.

" Too many files on disk!"

This message is displayed if there is not enough memory for AVPI to build its internal data structures. If you see this message, exclude some file extensions from the user-defined extensions list.

7.2 AVP Inspector for Web Servers™ Startup And Run-Time Messages

When AVP Inspector for Web Servers™ starts up the following messages may be displayed:

Disk subsystem configuration has been changed. Do you want to save the new configuration?

This message is displayed only when drive letters on your computer have been added or removed, for example after adding a new hard drive or creating or deleting a logical drive.

Cannot Create AVPI main window

This message is displayed if there is not enough system resources to open AVPI Main window.

7.3 Debugging registers test messages

AVPI performs a debugging registers test before beginning any checks. During normal operation (not under a debugger) the system should not have any hardware breakpoints set. The following messages may occur:

Hardware breakpoint detected at XXXX:XXXX

Ensure that no debuggers (like Turbo Debugger™, Soft ICE/W™ or CodeView™) are running when AVPI runs, and there are no hardware breakpoints left from your previous debugging sessions. If after you have done that you still keep getting this message where breakpoint segment address points to BIOS area (C000h - FFF0h) there could be a serious problem! Try removing the breakpoints by pressing the **"Remove"** button.

Cannot access debugging registers

This message may be displayed during the debugging registers test and may be caused by an active virus or a debugger that is running.

7.4 Other messages

The following messages are mostly debugging or diagnostic messages.

AVP Inspector for Web Servers requires AVPIChCk.DLL version X.XX or later to operate correctly. Please use AVPIChCk.DLL from AntiViral Toolkit Pro.

This message is displayed during AVP Inspector for Web Servers™ launch if the version of AVPIChCk.DLL currently installed is lower than X.XX. This is an AVP Inspector for Web Servers™ internal library.

AVP Inspector for Web Servers requires NKrnl32.DLL version X.XX or later to operate correctly. Please use NKrnl32.DLL from AntiViral Toolkit Pro.

This message is displayed during AVP Inspector for Web Servers™ launch if the version of NKrnl32.DLL (NKrnlNT.DLL) currently installed is lower than X.XX. This is an AVP Inspector for Web Servers™ internal library.

AVP Inspector for Web Servers requires NCCL32.DLL version X.XX or later to operate correctly. Please use NCCL32.DLL from AntiViral Toolkit Pro.

This message is displayed during AVP Inspector for Web Servers™ launch if the version of NCCL32.DLL currently installed is lower than X.XX. This is an AVP Inspector for Web Servers™ control elements library.

AVP Inspector for Web Servers requires NCA32.DLL version X.XX or later to operate correctly. Please use NCA32.DLL from AntiViral Toolkit Pro.

This message is displayed during AVP Inspector for Web Servers™ launch if the version of NCA32.DLL currently installed is lower than X.XX. This is an AVP Inspector for Web Servers™ disassembler and code analyzer library.

AVP Inspector for Web Servers requires NAVKVxD4.VxD version X.XX or later to operate correctly. Please use NAVKVxD4.VxD from AntiViral Toolkit Pro.

This message is displayed during AVP Inspector for Web Servers™ launch if the version of NAVKVxD4.VxD currently installed is lower than X.XX.

These last messages may appear if you have updated only the AVPI.EXE and AVPIChCk.DLL files. If so, update all other files as well, or reinstall AVPI.

8. Glossary

File Attributes
File characteristics: System file, Hidden File, Read Only File etc.

Absolute Sector
see: Sector

Blocker
see: Monitor

Interrupt Vector
An entry in the Interrupt Vectors Table. Points to the Interrupt Handler address.

Non-resident
see: Resident

Disassembler
A utility that derives assembly language code from executable code (the opposite to an assembler). Such utilities are valuable for debugging purposes as well as for virus analysis.

Disassembly
The process of creating assembly language code from executable code.

Distribution (Distribution copies)
Diskettes, CD-ROMs or copies thereof containing files from which a software application may be installed on to a computer.

EXE file header
Part of the structure of an EXE (Application) file which contains control data. It is located at the start of the EXE file and contains data for the operating system loader such as the length of the loadable module, register values, relocation table and so on.

Cluster
The unit of data storage on a logical drive. Consists of one or several logical drive sectors in a row. The cluster size for floppy drives is usually 1 or 2 sectors, for hard disks it may be up to 64 sectors.

Logical drive
A disk partition, containing a continuous block of disk sectors. A logical drive consists of a boot sector, FAT sectors, the root directory and data areas. Sectors in the data area are grouped into clusters. Logical drives are assigned letters (A:, B:, C: etc.) Within a single logical drive logical sector addressing is possible.

Logical sector
see: Sector

Monitor (Monitor program, Blocker)
A memory resident utility that detects "suspicious" actions of user programs such as the modification and renaming of executables (COM and EXE files), direct writes to disk, attempts to format the disk and so on. Having detected a "suspicious" function, the monitor program displays awarning or blocks execution of the intercepted function.

Interrupt
A signal which makes the processor stop execution of the current program and transfer control to an interrupt handler routine. The address of the interrupt handler is determined using the interrupt vector table. An interrupt may be initiated either by software or hardware.

Ghost (Ghost Viruses)
Viruses that take extra measures to avoid detection and analysis. They have no signatures, i.e. they have no single constant fragment of code that can be used as a means of identification. In most cases two instances of the same Ghost Virus will have no bytes in common. This is achieved by encrypting the main virus body and modifying the decryption code.

Fake Bad Cluster
Each cluster of a logical drive is marked in the FAT as free, occupied or bad. A cluster is considered bad if it contains one or more bad sectors. Such a cluster is not used by DOS. A fake bad cluster is a normal cluster (not containing bad sectors) which is marked as bad in the FAT. It is possible to tell fake bad clusters from genuine bad clusters by repeatedly reading the sectors included in the cluster. If there are no errors during this process the cluster is fake. Some viruses may mark good clusters as bad and then use them for their own purposes.

Resident (TSR – Terminate and Stay Resident)
Executable programs may be resident or non-resident. A resident program leaves

code in computer memory after it terminates. This code is typically installed as an interrupt handler and is executed when an interrupt occurs.

Sector
The smallest physical unit of storage on disk. A disk is divided into sectors when it is formatted. Each sector can be uniquely addressed. A sector may have both a physical (relative to the start of the disk, accessed using BIOS calls) and a logical (relative to the start of a partition, accessed using DOS calls) address. The sector size is usually 512 bytes.

Stealth
Stealth viruses (invisible viruses) are viruses that intercept DOS calls so that when an infected file or sector is accessed, the evidence of infection can be hidden from the calling program. Stealth viruses may employ other techniques too in order to defeat resident anti-virus monitors. Examples of stealth viruses are "V-4096", "Fish#6" and "Brain".

Interrupt Vectors Table
A table in memory containing the addresses of interrupt handler routines. It is placed in the lowest memory addresses (0000:0000 - 0000:03FF) and contains 256 addresses (interrupt vectors) of 4 bytes each.

Relocation Table
see: EXE file

Trojan Horse
A program or routine that performs destructive actions but which masquerades as something useful.

File
The logical unit of data storage on disk. A files may contain data of any type: programs, databases, text, etc. A file has attributes such as the file name, file size (the number of bytes of data it contains) and date and time of last modification.

Physical Sector
see: Sector

Backup
Copies of software and data made on a backup medium such as tape or removable disk, taken as a precaution against loss of the software or data on the

computer hard disk.

BIOS (Basic Input-Output System)
Built-in software included with your computer. It performs functions such as testing the hardware at start-up, and launching the operating system boot procedure. It also provides the primary interface to hardware such as the screen, disks, printers, etc. The BIOS code is stored in ROM.

Boot Sector
The first sector of a logical drive (also the first physical sector on floppies). It contains the operating system loader code which is executed during boot-up.

DOS (Disk Operating System)
One of many operating systems available for IBM-compatible PCs. It is loaded from disk and provides a user interface (command prompt) as well as file access functions for use by applications.

FAT (File Allocation Table)
A data table stored on each logical drive, immediately following the Boot Sector, which contains information about the location of all the disk clusters in each file. It also contains data to identify the bad clusters on the logical drive.

MBR (Master Boot Record)
The first physical sector of the hard disk. It usually contains a small loader routine and the disk partition table. The loader routine analyzes the disk partition table, selects an active logical drive from it, loads the boot sector of this drive into memory and then executes it.

TSR
see: Resident

COM File
A simple form of executable file used for small MS-DOS programs which usually occupy a single segment of RAM.

EXE File
A more complex form of executable file used for both DOS and Windows programs. There are several different types. Information about the program is contained within the EXE file header, such as instructions on how to load the file into memory.

OVL File
A file containing executable code which may be used by a calling program. It often has a COM or EXE file structure.

SYS File
A system device driver file. It is loaded into memory when DOS initializes after boot-up. System files are loaded as instructed by DEVICE commands in the file CONFIG.SYS which are actioned during boot-up.

9. Kaspersky Lab Ltd.

Kaspersky Lab

Kaspersky Lab Ltd. is a fast growing international privately owned software development company with offices in Moscow (Russia) and Cambridge (UK). Having started the business in 1992 Kaspersky Lab concentrates its efforts on the development, marketing and distribution of world-leading anti-virus technologies and computer software.

Weekly anti-virus database updates

Every week up to 200 new viruses appear. Your system is at risk from new viruses until your anti-virus database is updated to include them. AVP's database is updated weekly, so AVP provides unbeatable protection. You may update your antiviral databases via Internet and BBS.

Immediate response to new virus attack

When new types of virus appear, exploiting new operating system features or security loopholes, AVP, using the most advanced technologies, will neutralize it fastest. In June, 1998 Kaspersky Lab took just 3 hours to develop *the world's first* effective cure module for the Win95.CIH ("Chernobyl") virus.

Personal attention to every client

When a registered user reports an unknown virus, Kaspersky Lab will develop a personal cure module within 48 hours. This module will be provided directly to all customers in the next weekly update.

Information support

Kaspersky Lab produces AVP *Virus Encyclopedia* (http://www.viruslist.com) – a unique resource containing information about more than 15,000 viruses available to all AVP users.

Integrated network solution for the whole enterprise

The AVP product family comprises a complete set of tools that provide virus protection for both workstations and network servers, and the means to control it. AVP is a *comprehensive integrated* system of anti-virus protection:

- For all corporate network components: workstations, servers, mail systems, firewalls;

- For most popular operating systems;
- Includes powerful and flexible management tools

Year 2000 compliant

Kaspersky Lab is the first anti-virus software vendor to certify its products for year 2000 compliance in an independent testing lab. This certificate confirms that all AVP family products will work correctly after year 2000.

Certificates

AVP for Windows is certified by Microsoft's Testing Lab and carries the "Designed for Windows 95/NT" and "Designed for Windows 98/NT" logos. AVP is checked for 100% detection of viruses "In-the-Wild" by leading anti-virus testing lab - West Coast Labs. AVP has the "CheckMark" certificate. The International Computer Security Association (ICSA) certifies AVP. State committee certifies AVP for the year 2000 compliance. The certificate corresponds with VTU 115-006-1999 standard, which is similar to DISC PD2000-1 standard of the British Standard Institute.

Other Kaspersky's Lab AntiViral Products

All the AVP software products use the same antivirus bases (updates) what is very convenient especially for users applying AVP under several platforms.

AntiViral Toolkit Pro for Windows 95/98/NT Workstation

AVP for Windows 95/98/NT Workstation is a completely 32-bit application that corresponds to a powerful integrated antivirus system comprising **AVP Scanner** and resident **AVP Monitor**. The AVP for Windows 95/98/NT built-in AVP Updates engine enables a user to *automatically* update the antivirus bases via the Internet or from a network storage. There are several editions of the product: AVP Platinum edition, AVP Gold edition, AVP Silver edition and AVP Lite edition.

AntiViral Toolkit Pro for DOS

AVP for DOS 32 (AVPDOS32) is a 32-bit application specially developed for the DOS 32 environment. The package contains an antivirus scanner and the setting program. Both the components are armed with interfaces appropriate for the environment.

AntiViral Toolkit Pro for Novell NetWare

AVP for Novell NetWare (AVPN) is an antivirus system for the Novell NetWare computer network. AVPN performs scanner and filter tasks permanently supervising server files.

AntiViral Toolkit Pro for Windows NT Server

AVP for Windows NT Server is designed to build a reliable antivirus protection system on the file and application servers operating under Microsoft Windows NT Server.

AntiViral Toolkit Pro for OS/2

AVP for OS/2 is a 32-bit application specially designed to operate in the IBM OS/2 environment. This package scanner and monitor are the first antivirus tools in the world armed with the OS/2 Presentation Manager user interface.

AntiViral Toolkit Pro for Linux

AVP for Linux is a 32-bit application specially designed for the Intel platform UNIX environment. The package is armed with an antivirus scanner similar to the one of AVP for DOS 32.

AntiViral Toolkit Pro Inspector

AVP Inspector enables a user to protect workstations operating in the Windows environment from viruses. Inspector checks files, folders and disk sectors for any modification that corresponds to a virus manifestation.

AntiViral Toolkit Pro Control Center (AVPCC)

AVP Control Center enables a user to control all the other components of the AVP package. AVPCC provides the ability to adjust and schedule AVP virus checking units automatic starts and the bases updates. This AVP integrated shell utility operates under Microsoft Windows 95, Windows 98 and Windows NT.

AntiViral Toolkit Pro Network Control Center (AVPNCC)

AVP Network Control Center enables a network administrator to control AVP components (to install and update the components, to schedule AVP units automatic start, to adjust their reporting mode and etc.) on any remote workstation of the network.

AntiViral Toolkit Pro Virus Encyclopedia (AVPVE)

AVP Virus Encyclopedia is an electronic HTML document. AVPVE details on almost all the worldwide ever detected viruses (more than 5000 pieces), their classifications, detection and deletion approaches, their operation concepts, their manifestations and after-effects of the virus infection. The product also demonstrates graphical and sound effects produced by viruses. AVPVE is FREE! It may be downloaded through the Internet at the following addresses: http://www.avpve.ru or http://www.viruslist.com.

Kaspersky Lab Contact Information

If you have any questions, comments or suggestions you may refer to our distributors listed in your AVP README.TXT file or directly to Kaspersky Lab. We will be glad to consult you on any matters related to our product by phone or e-mail and all your recommendations and suggestions will be thoroughly reviewed and considered.

Our contact information:

Address:	:	10, Geroyev Panfilovtcev Street, 123363, Moscow, Russia, Kasperskly Lab
Phone:	:	+7 (095) 948-43-31 - Sales Department, +7 (095) 495-03-00 Technical Support +7(095)948-56-50 Marketing and Advertising Department
Fax:	:	+7 (095) 948-4331
BBS:	:	+7 (095) 948-6333, +7 (095) 948-3601 (clock round service)
E-Mail:	:	globalsale@avp.ru – distribution related matters support@avp.ru Technical Support newvirus@avp.ru - Antiviral Laboratory (information about viruses only) info@avp.ru - Marketing and Advertising Department
FidoNet:	:	2:5020/156;
WWW:	:	http://www.avp.ru, http://www.viruslist.ru